

The University of Chicago

CONSTRUCTION OF NON-ABELIAN
FIELDS WITH PRESCRIBED
ARITHMETIC

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS
DECEMBER, 1941

By
ANATOL RAPOPORT

CHICAGO, ILLINOIS

1944

The University of Chicago

**CONSTRUCTION OF NON-ABELIAN
FIELDS WITH PRESCRIBED
ARITHMETIC**

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS
DECEMBER, 1941

By
ANATOL RAPOPORT

CHICAGO, ILLINOIS

1944

TABLE OF CONTENTS

	Page
INTRODUCTION	1
 I. ALGEBRAIC STRUCTURE	
1. Lattice of subfields	3
2. Conditions of extensibility	6
3. Construction of extensible fields	10
4. Construction of the non-abelian field	13
 II. ARITHMETIC STRUCTURE	
5. Arithmetic of cyclic extensions	14
6. Arithmetic of an extensible field	15
7. Arithmetic of the non-abelian field	22
8. The general existence theorem	27



CONSTRUCTION OF NON-ABELIAN FIELDS WITH PRESCRIBED ARITHMETIC

INTRODUCTION

An imbedding problem in the theory of algebraic extensions of fields is concerned with the existence and construction of an algebraic extension L of a given base field F such that the relative Galois group of L/F is isomorphic to a given group G and such that L contains a given extension K of F . If $K = F$, the imbedding problem reduces to the inverse problem of Galois Theory.

It is known that some questions of the general inverse problem of Galois Theory can be immediately answered. For example given a finite group G , it is always possible to construct two fields F and L such that the Galois group of $L/F = G$. On the other hand the question whether algebraic extensions with a given Galois group which is not the identity group exist over an arbitrary field must be answered in the negative. Obviously no such extensions exist, for example, over an algebraically closed field. The question whether algebraic extensions with an arbitrary prescribed group exist over any given finite algebraic number field has not yet been answered in general. However several interesting special imbedding problems of this kind have been solved.

Usually such problems are solved by exhibiting necessary and sufficient conditions on the field K such that the field L exists.

In this paper the field F is an arbitrary algebraic number field subject only to the condition that it contains primitive

p -th roots of unity where p is an odd prime. The field K is an abelian extension of type (p, p) over F . This field K is to be imbedded in a field L , non-abelian of degree p^3 over F . We find necessary and sufficient conditions on K such that the problem is solvable and indicate the construction of all such fields K . The construction of all fields L is then also shown.

In the second part of the paper we consider the possible arithmetics of L with respect to a given finite set of prime ideals $\mathcal{P}_1$ ($i = 1, \dots, n$) of F . By an arithmetic of L with respect to $\mathcal{P}$ we mean the manner of factorization of $\mathcal{P}$ in the various subfields of L . Since the number of subfields of L over F is finite, and since a prime ideal $\mathcal{P}$ can factor only in a finite number of distinct ways in each subfield, it follows that only a finite number of arithmetics of L with respect to $\mathcal{P}$ are conceivable. We show that apart from those arithmetics which are excluded by the considerations of Hilbert's arithmetic theory of fields, all the arithmetics of L with respect to the set $\mathcal{P}_1$ are realizable where $\mathcal{P}_1$ does not divide p ($i = 1, \dots, n$). We prove this by exhibiting an actual construction of L such that L/F has the desired group and the desired arithmetic in each case.

I. ALGEBRAIC STRUCTURE

1. The lattice of subfields.—Let F be a finite algebraic number field containing primitive p -th roots of unity ζ , where p is an odd prime. We wish to discuss the algebraic structure of non-abelian extensions L of degree p^3 over F . There are exactly¹ two distinct non-abelian groups of order p^3 . Their structure is given by the following relations.

$$(1) \quad G = \{A, B\} \quad \text{with } A^{p^2} = B^p = 1, \quad BA = A^{p+1}B, \quad A^pB = BA^p$$

and

$$(1') \quad G' = \{A, B, C\} \quad \text{with } A^p = B^p = C^p = 1, \quad BA = CAB,$$

$$AC = CA, \quad BC = CB.$$

In both cases the group under consideration has the abelian group of type (p, p) as factor group. In fact,

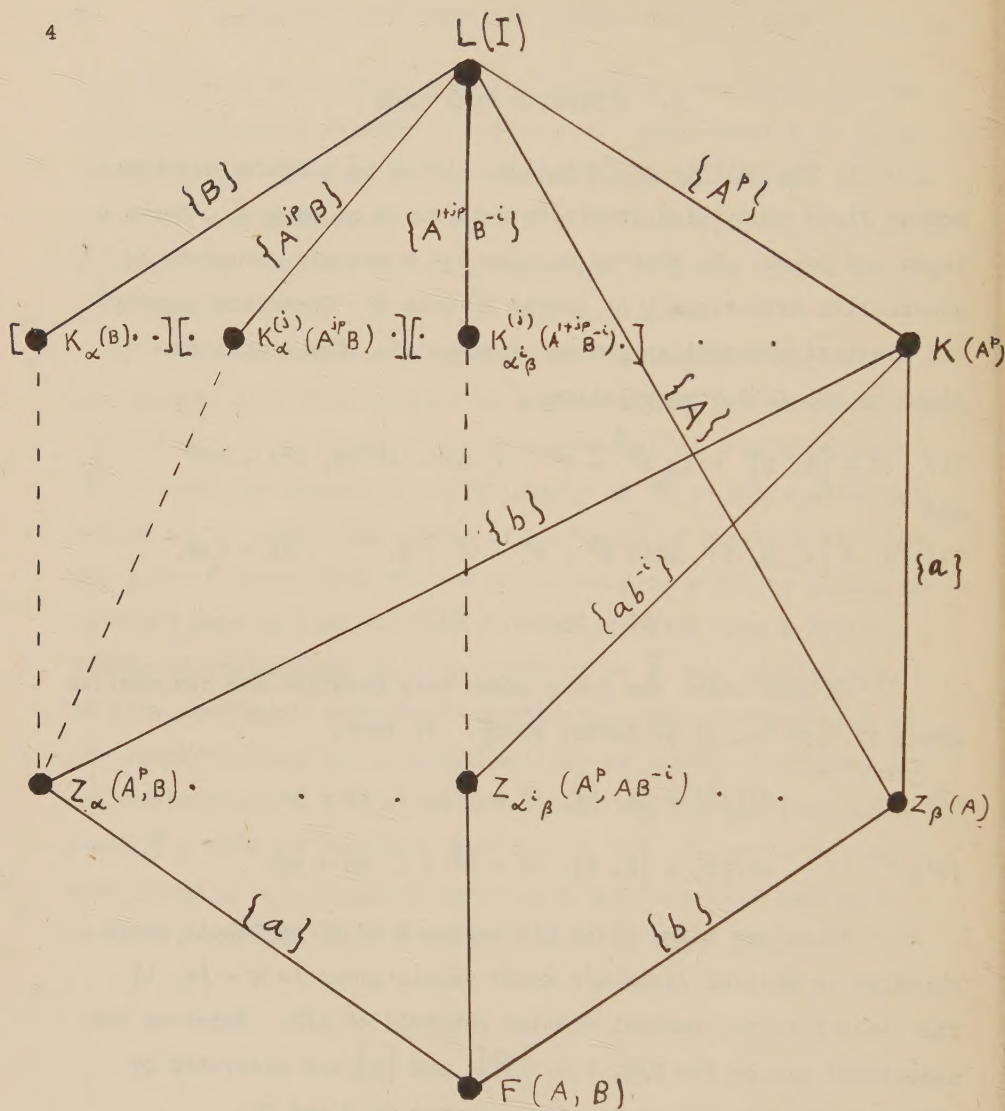
$$(2) \quad G/\{A^p\} = \{a, b\}; \quad a^p = b^p = 1, \quad ab = ba,$$

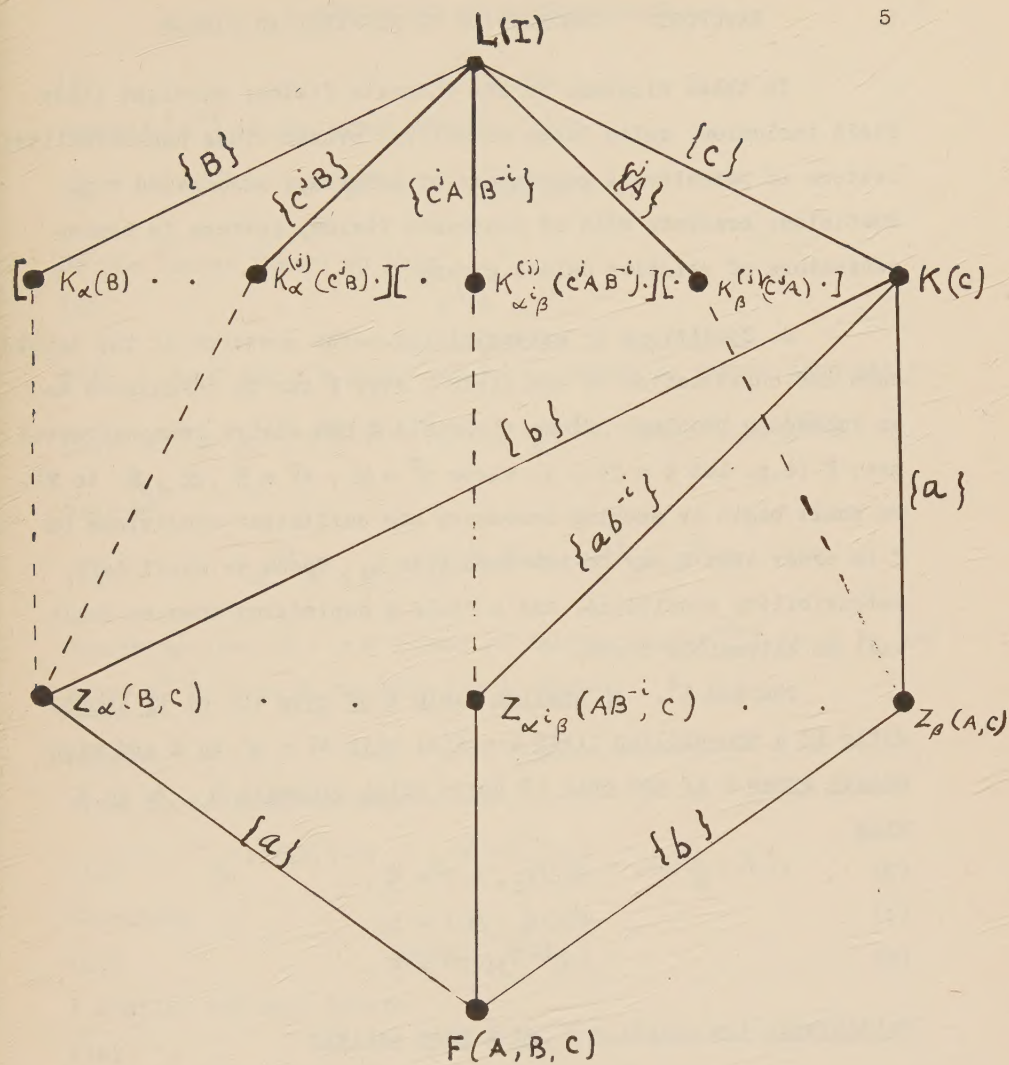
$$(2') \quad G'/\{C\} = \{a, b\}; \quad a^p = b^p = 1, \quad ab = ba.$$

Thus, any fixed field L/F having G of G' as Galois group contains an abelian field K/F whose Galois group is $g = \{a, b\}$. The field K is the maximal abelian subfield of L/F . Moreover the associated groups for L/K , i.e. $\{A^p\}$, and $\{C\}$ are generated by elements lying in the respective centrums of G and G' .

The following diagrams of the lattices of subfields gives the complete algebraic structure of L over F having groups G and G' respectively.

¹H. Zassenhaus, Lehrbuch der Gruppentheorie, 1937, pp. 114.





In these diagrams points indicate fields; straight lines field inclusion, solid lines normality; broken lines non-normality; letters in parentheses generators of subgroups associated with subfields; brackets sets of conjugate fields; letters in braces generators of relative Galois groups.

2. Conditions of extensibility.--The question of the existence and construction of the field L over F can be formulated as an imbedding problem. Since the field K can always be constructed over F (e.g. let $K = F(x, y)$ where $x^p = \alpha$, $y^p = \beta$, α, β in F), we shall begin by seeking necessary and sufficient conditions on K in order that K may be imbedded into L . These we shall call extensibility conditions, and a field K satisfying them we shall call an extensible field.

THEOREM 1². An abelian field K of type (p, p) is imbeddible in a non-abelian field $L = K(z)$ with $z^p = \gamma$ in K and with Galois group G if and only if there exist elements λ, μ in K with

$$(3) \quad N(K/\mathbb{Z}_\beta; \lambda) = \zeta,$$

$$(4) \quad N(K/\mathbb{Z}_\alpha; \mu) = 1,$$

$$(5) \quad \lambda^{b-1} \mu^{1-a} = \zeta.$$

Furthermore the quantity γ of K must satisfy

$$(6) \quad \gamma^{a-1} = \lambda^p,$$

$$(7) \quad \gamma^{b-1} = \mu^p.$$

Proof. Let L be a normal extension of F with $G = \{A, B\}$ as Galois group. Then $L = K(z)$ with $z^p = \gamma$ in K . Furthermore

²An alternate proof may be given by appealing to a theorem of R. Brauer; cf. R. Brauer, Über die Konstruktion der Schiefkörper, Journal für die reine und angewandte Mathematik, vol. 168 (1932), pp. 44-64.

$$(8) \quad z^{A^p} = \zeta z$$

because $\{A^p\}$ is the group of L/K . Also

$$(9) \quad z^{B^p} = z \quad \text{since } B^p = 1.$$

By the Kummer Theory we have

$$(10) \quad z^A = \lambda z^r$$

with λ in K and r a prime modulo p . Hence by direct computation

$$(11) \quad z^{A^p} = \lambda^{(A^p - r^p)(A-r)^{-1}} z^{rp} = \lambda^{(A^p - r^p)(A-r)^{-1}} z^{r \cdot z^{p-r}}.$$

Thus z^{A^p}

$$(12) \quad z^{A^p} = \zeta z = \lambda^{(A^p - r^p)(A-r)^{-1}} z^{r \cdot z^{p-r}}.$$

Observing that $r^p - r \equiv 0 \pmod{p}$ implies that $z^{r^p - r}$ is in K , and hence z^{r-1} is in K , we have $r = 1$, whence

$$(13) \quad z^A = \lambda z.$$

Since λ is in K , we have

$$(14) \quad \lambda^{(A^p - 1)(1-A)} = \lambda^{(a^p - 1)(1-a)} = N(K/Z_\lambda; \lambda).$$

Therefore

$$(15) \quad N(K/Z_\lambda; \lambda) = \zeta.$$

A similar argument proves

$$(16) \quad z^B = \mu z$$

with μ in K and $N(K/Z_\mu; \mu) = 1$. Raising equations (13) and (16) to the p -th power, we obtain (6) and (7). To prove (5), we apply the automorphisms of G to (13) and (16) respectively and get

$$(17) \quad z^{AB} = (z^B)^A = (\mu z)^A = \mu^A z^A = \mu^a \lambda z,$$

$$(18) \quad z^{BA} = (z^A)^B = (\lambda z)^B = \lambda^B z^B = \lambda^b \mu z,$$

But $BA = A^pAB$ gives $z^{BA} = (z^{AB})A^p = (\mu^a \lambda z)^{A^p} = \mu^a \lambda \zeta z$.
Hence $\lambda^b \mu = \mu^a \lambda \zeta$ and $\lambda^{b-1} \mu^{1-a} = \zeta$ as desired.

For proof of the converse suppose that there exist in K quantities λ, μ satisfying (3), (4) and (5). Then
 $N(K/Z_\beta; \lambda^p) = N(K/Z_\alpha; \mu^p) = 1$. Therefore

$$(19) \quad \lambda^p = \lambda^{a-1}$$

$$(20) \quad \mu^p = \mu^{b-1}$$

with λ, μ in K . Raising (5) to the p -th power, we find

$$(21) \quad \lambda^{(a-1)(b-1)} \mu^{(b-1)(1-a)} = 1.$$

Consequently

$$(22) \quad (\lambda \mu^{-1})^{(a-1)(b-1)} = 1.$$

By a theorem of Nakayama³

$$(23) \quad \lambda \mu^{-1} = \sum_{\alpha} \sum_{\beta}$$

with $\sum_{\alpha}$ in Z_{α} , $\sum_{\beta}$ in Z_{β} . Substituting $\mu^{-1} \sum_{\alpha} \sum_{\beta}$ for λ into (19) and noting that $\sum_{\alpha}^{b-1} = 1$, we obtain

$$(24) \quad \lambda^p = (\mu \sum_{\alpha})^{a-1},$$

$$(25) \quad \mu^p = (\mu \sum_{\alpha})^{b-1}.$$

Thus $\mu \sum_{\alpha} = \gamma$ is a solution of (6) and (7). Finally we note that the relations $z^A = \lambda z$, $z^B = \mu z$, define automorphisms A and B of L over F . A direct computation shows that these automorphisms generate precisely the group G . Therefore L/F has the desired group. This proves the theorem.

THEOREM 1'. An abelian field of type (p, p) is embeddible in a non-abelian field $L = K(z)$ with $z^p = \gamma$ in K and with group G' if and only if there exist elements λ, μ in K with

³T. Nakayama, solution of problem 222, Jahresbericht der Deutschen Mathematiker Vereinigung, vol. 48 (1938), p. 10.

$$\begin{aligned}(3') \quad & N(K/Z_\beta; \lambda) = 1, \\(4') \quad & N(K/Z_\alpha; \lambda) = 1, \\(5') \quad & \lambda^{b-1} \lambda^{1-a} = \zeta.\end{aligned}$$

The proof is similar to that of Theorem 1. Instead of equations (8) and (9), we have

$$\begin{aligned}(8') \quad & z^C = \zeta z, \\(9') \quad & z^{A^p} = z^{B^p} = z,\end{aligned}$$

leading by analogous arguments to

$$(15') \quad N(K/Z_\beta, \lambda) = 1$$

and the theorem follows immediately.

DEFINITION. If a field Z is cyclic of degree p over F , so that $Z = F(x)$ with $x^p = a$ in F , we shall call the quantity a the generator of Z over F .

THEOREM 2. Let $L = K(z)$ with $z^p = \gamma$ in K be any extension of F with group G . Then the generator of each field L over K can always be selected in Z .

Proof. By Theorem 1 we have $\gamma^{b-1} = \lambda^p$ with $N(K/Z_\alpha; \lambda) = 1$. Then $\lambda = m^{b-1}$ with m in K . Hence $\gamma^{b-1} = \lambda^p = (m^p)^{b-1}$ and $\gamma = m^p T_\alpha$ with T_α in Z_α . But for the generator of the same field L over K we can choose the quantity $\gamma_0 = \gamma m^{-p} = T_\alpha$ in Z_α . This proves the theorem.

THEOREM 2'. Let L have group G' over F . Then γ may be chosen either in Z_α or in Z_β .

Proof. In this case the norms of both λ and λ are unity, and the argument of Theorem 2 may be applied to either.

COROLLARY 1. If γ is chosen in Z_α , then λ is a p -th root of unity.

Proof. We have by Theorem 1 $\gamma^{b-1} = \mathcal{M}^p$. But by hypothesis γ is in Z_α . Thus $\gamma^{b-1} = \mathcal{M}^p = 1$ and $\mathcal{M}$ is a p -th root of unity.

COROLLARY 1'. If γ is chosen in Z_α , then $\mathcal{M}$ is a p -th root of unity; if it is chosen in Z_β , then λ is a p -th root of unity.

COROLLARY 2. The field K is extensible to L with group G if and only if there exists in K a quantity λ satisfying the following relations

$$(26) \quad N(K/Z_\beta; \lambda) = \zeta,$$

$$(27) \quad \lambda^{b-1} = \zeta.$$

Proof. If K contains λ satisfying (26) and (27), we take $\mathcal{M} = 1$ and note that λ and $\mathcal{M}$ satisfy (3), (4) and (5). The corollary then follows by Theorem 1.

Conversely if K is extensible, choose γ in Z_α , and conclusion follows by Corollary 1.

COROLLARY 2'. The field K is extensible to L with group G' if and only if K contains an element λ such that $N(K/Z_\beta; \lambda) = 1$ and $\lambda^{b-1} = \zeta$; or K contains an element $\mathcal{M}$ such that $N(K/Z_\alpha; \mathcal{M}) = 1$ and $\mathcal{M}^{1-a} = \zeta$.

3. Construction of extensible fields.---In order to study below the problem whether the field K with a given arithmetical structure can be extended, we shall obtain conditions on α and β , the generators of the cyclic subfields of K over F , which shall insure extensibility of K to L .

LEMMA 1. Let $Z = F(x)$ with $x^p = a$ in F be a cyclic extension of degree p over F with generating automorphism S . Then the cyclic algebra $\mathcal{U} = (Z/F, S, b)$ is similar to the cyclic

system⁴ $(F(y)/F, \bar{S}, a^{-1})$, where $\bar{S}$ is the generating automorphism of the cyclic semi-field $F(y)/F$ with $y^p = b$.

Proof. Suppose the algebra $(Z/F, S, b)$ is given by the relations

$$(28) \quad \begin{aligned} u^p &= a, \\ v^p &= b, \\ uvu^{-1} &= v. \end{aligned}$$

Now let $V = u^{-1}$, $U = v$. Then $V^{-1}UV = uvu^{-1} = \zeta v = \zeta U$, $U^p = b$, $V^p = a^{-1}$. Hence the algebra $\mathcal{K}^{-1}$ may be generated by V and U with the above relations. The roots of $U^p = b$ generate over F a cyclic semi-field $(F^p b/F) = F(U)/F$ with generating automorphism $\bar{S}$. Then $(F^p b/F, \bar{S}, a^{-1})$ is similar to $\mathcal{K}$. Thus the theorem is proved.

COROLLARY 3. The algebra $\mathcal{K} \sim 1$ if and only if $(F^p b/F, \bar{S}, a^{-1}) \sim 1$, in other words we have the relation⁵
 $b = N(F(x)/F; B)$ with B in $F(x)$ where $x^p = a$ if and only if
 $a = N(F(y)/F; A)$ with A in $F(y)$ where $y^p = b$.

In the following constructions we shall show that either Z_α or Z_β may be selected freely. When one is selected, the generator of the other must satisfy certain norm conditions.

THEOREM 3. Let $Z_\alpha = F(x)$ with $x^p = \alpha$ an arbitrary quantity (not a p -th power) of F . Then $K = (Z_\alpha \cup Z_\beta)$ is extensible to L with group G if and only if $Z_\beta = F(y)$ with $y^p = \beta$ in F and
 (29)
$$\beta = \zeta N(Z/F, B)$$

⁴For the definition of a cyclic system, cf. A. A. Albert, Structures of Algebras, 1939, p. 88.

⁵We denote the norm of an element B taken from $F(x)$ to F by $N(F(x)/F; B)$.

with B in Z_α .

Proof. Let K be extensible. Then by Corollary 2 there exists in K a quantity λ such that $N(K/Z_\beta; \lambda) = \zeta$ and $\lambda^{b-1} = \zeta$. Then $\lambda = yB_\alpha$ with B_α in Z_α since $Z_\alpha(\lambda) = K$ and $y^{b-1} = \zeta$. Furthermore $N(K/Z_\beta, B_\alpha) = N(Z_\alpha/F, B_\alpha)$. Therefore $\zeta = \beta N(Z_\alpha/F, B_\alpha)$ because y lies in Z_β and consequently $\beta = \zeta N(Z_\alpha/F, B)$ where $B = B_\alpha^{-1}$.

Conversely suppose $\beta = \zeta N(Z_\alpha/F, B)$. Then the quantity $\lambda = yB^{-1}$ satisfies (26) and (27), and K is extensible by Corollary 2.

THEOREM 4. Let $Z = F(y)$ with $y^p = \beta$ in F . Then $K = (Z_\alpha \cup Z_\beta)$ is extensible to L if and only if $Z_\alpha = F(x)$ with $x^p = \alpha$ in F where α is a norm of a quantity in $F(\sqrt[p]{\beta\zeta^{-1}})$ over F .

Proof. Again as in Theorem 3 if K is extensible, we have by the proof of that theorem $\beta = \zeta N(Z_\alpha/F, B)$. Then the quantity $\beta\zeta^{-1}$ is a norm of a quantity in Z_α over F . By Lemma 1, α is then a norm of a quantity in $F(\sqrt[p]{\beta\zeta^{-1}})$ over F .

The converse is proved as in the preceding theorem.

By exactly analogous arguments we obtain

THEOREM 3'. Let α be arbitrary. Then K is extensible to L with group G' if and only if β is a norm of a quantity in Z_α over F .

THEOREM 4'. Let β be arbitrary. Then K is extensible to L with group G' if and only if α is a norm in Z_β/F .

We observe that Theorems 3 and 4 (3' and 4') are actually equivalent. Therefore in order to construct a field K which is extensible, it suffices to determine β for a given α (or as an alternative to determine α for a given β). The fields K obtained

by either construction represent all extensible fields of type (p, p) over F . In the sequel we shall always select α first and then seek a β satisfying the above conditions.

4. Construction of the non-abelian field.

THEOREM 5. Let $L_0 = K(z)$ with $z^p = \gamma_0$ in K be a normal field of degree p^3 over F and with Galois group G . Then the set of fields (L_c) where $L_c = K(z)$ with $z^p = \gamma_0 c$ where $c \neq 0$ ranges over all the quantities of F is the set of all normal extensions L of degree p^3 over F with Galois group G .

Proof. The fields L are cyclic of degree p^2 over Z_β by section 1. Then by a theorem of Albert, the set of all fields L is the set $\{L_c\}$ where $L_c = K(z)$ with $z^p = \gamma_0 c$, where c ranges over all the non-zero quantities of Z_β . But by Theorem 2 the generators γ_0 of L_0 and $\gamma_0 c$ of L_c can be chosen in Z_α . Hence c is in Z and therefore in the intersection of Z_α and Z_β , in other words in F .

THEOREM 5'. Theorem 5 holds when the Galois group of L over F is G' .

Proof. Let L be an arbitrary field from the set L_c . Then the generator of L over F is $\gamma_0 c$ with c in F . Since c is invariant under the automorphisms of K and since γ_0 generates a field L over K , the quantity $\gamma_0 c$ satisfies the conditions of Theorem 1. Conversely, let $\gamma_0 c$, c in K be a generator of a field L . Then by Theorem 2' $\gamma_0 c$ may be chosen either in Z_α or in Z_β . Let $\delta_\alpha c$ be in Z_α and $\delta_\beta c$ be in Z_β , where δ_α is a generator of L_0 in Z_α and δ_β is a generator of L_0 in Z_β . Then c is in Z_α and in Z_β and hence in F .

The above theorems give the construction of all fields L , once the abelian subfield K of L has been constructed.

II. ARITHMETIC STRUCTURE

5. Arithmetic of cyclic extensions.--Let P stand for any prime ideal of F , so that $P \nmid p$, p a given rational prime.

We now wish to examine the possible factorizations of a prime ideal P of F in the various subfields of L . We should like to restate some results from the theory of cyclic fields.

Let $Z = F(x)$ with $x^p = a$ in F be a cyclic extension of degree p over F . Suppose that P is a prime ideal of F which is relatively prime to the degree p . Then the factorization⁶ of P in F can be described by means of the P -adic closure $\bar{F}$ of F . The multiplicative group $\bar{F}^\times$ of $\bar{F}$ can be generated by a prime element π_0 for P and a primitive $(q-1)$ st root of unity ω_0 where q is the absolute norm of P . Each element b of F has the form

$$(30) \quad b = \pi_0^r \omega_0^s u$$

where $u \equiv 1 \pmod{P}$. Since P is prime to p , each unit $u \equiv 1 \pmod{P}$ is equal to v^p with $v \equiv 1 \pmod{P}$ in F . The elements π_0 and ω_0 may be replaced by elements π, ω in F with $\pi\pi_0^{-1} \equiv 1 \pmod{P}$ $\omega \equiv \omega_0 \pmod{P}$ in $\bar{F}$. Then the residues modulo p of r and s in (30) are not changed. We may thus write

$$(31) \quad b = \pi^r \omega^s u_1$$

where the element u_1 is a p -th power of an element in $\bar{F}$. The factor group $\bar{F}^\times / \bar{F}^{p^\infty}$ is abelian of the type (p, p) .

⁶For the sequel see, e.g., K. Hensel, Die Verallgemeinerung des Legendreschen Symbols für allgemeine algebraische Körper, Journal für reine und angewandte Mathematik, vol. 147 (1916), pp. 233-248.

LEMMA 2. The factorization of P in Z/F is determined by the following conditions.

- (i) P is totally decomposed if and only if a is in $(\bar{F}')^p$.
 (ii) P is inert if and only if $a\omega^{-1}$ is in $(\bar{F}')^p$ for some $1 \not\equiv 0 \pmod{p}$.
 (iii) P is completely ramified if and only if $a\omega^{-j} \eta^{-k}$ is in $\bar{F}'$ for some $k \not\equiv 0 \pmod{p}$ and an arbitrary j .

In the sequel P is to be a fixed prime ideal of F . As a tool for the following constructions let Q_1, Q_2 be any two prime ideals distinct from P ; and ξ_1, ξ_2 the maps in F of the corresponding primitive roots of unity contained in the Q -adic closures $\bar{F}_{Q_1}, \bar{F}_{Q_2}$ of F . Further $P_\alpha, P_\beta, P_K, P_L$ shall denote prime ideals in the fields Z_α, Z_β, K, L dividing P . The corresponding closures shall be denoted by $\bar{Z}_\alpha, \bar{Z}_\beta$. etc. We shall also denote by α the conductor⁷ of Z over F .

6. Arithmetic of an extensible field.

DEFINITION. We shall call a chain of subfields of L over F a Hilbert series⁸ if its members are the decomposition, inertial, and ramification fields of a prime ideal in L .

We shall restrict the class of prime ideals in L to those which are prime to p . Then the Hilbert series do not contain subfields belonging to higher ramifications. The field L is then always the ramification field and must be cyclic over the inertial field. Moreover, the latter is cyclic over the decomposition field.

Each Hilbert series for L/F induces a corresponding Hilbert series for L/K and one for K/F . The latter belongs to the prime

⁷H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, 1930, Part II, p. 3.

⁸Cf., e.g., H. Hasse, op. cit., Part I.

ideal of K which is the intersection of the given prime ideal of L with K .

We wish to investigate the existence of L/F which realizes an abstractly possible Hilbert series for a given prime divisor in L of a given prime ideal P of F . For the solution of the problem we first consider the induced problem for K/F . In other words, we aim to construct an extensible field K of type (p, p) over F for a given P and any given Hilbert series of K/F which is possible for P .

Any factorization of P in K in turn induces factorizations in Z_α and Z_β . Of these there are exactly nine distinct cases abstractly possible, since P may conceivably decompose, remain inert or ramify in each field independently. We shall therefore examine these nine cases.

Case 1. Full decomposition of P in Z_α and in Z_β .

This case is always possible.

For the construction of $K = Z_\alpha \cup Z_\beta$ we shall employ

Theorem 3. Let α in F satisfy the congruences

$$(32) \quad \alpha \equiv 1 \pmod{P},$$

$$(33) \quad \alpha \equiv \xi_1 \pmod{Q_1},$$

$$(34) \quad \alpha \equiv 1 \pmod{Q_2}.$$

These are additive congruences and have a solution by the Chinese Remainder Theorem. Then by (33) $Z_\alpha = F(\alpha)$ is a proper extension, for $\alpha \not\equiv 1 \pmod{P}$ in F . Furthermore by (32) α is in $(\overline{F})^P$ and consequently P decomposes in Z_α by Lemma 2. Next let satisfy the congruences⁹

⁹These congruences are multiplicative; however it will suffice in the sequel to consider additive congruences. H. Hasse, op. cit.

$$\begin{aligned}
 (35) \quad & \beta \equiv 1 \pmod{P}, \\
 (36) \quad & \beta \equiv \zeta \pmod{\alpha}, \\
 (37) \quad & \beta \equiv \varepsilon_2 \pmod{Q_2}.
 \end{aligned}$$

Also these congruences have a solution since P , Q_2 and α are relatively prime in pairs. Then by (37), Z_β is a proper extension. Also $Z_\alpha \neq Z_\beta$ since $\alpha\beta^{-1} \neq 1$ in F by (34) and (37). Furthermore P decomposes in Z_β by (35). Finally¹⁰ K is extensible by (36). Therefore K is a desired field.

Case 2. Decomposition in Z_α , inertness in Z_β .

This case is always realizable.

Let α satisfy (32), (33) and (34), and β satisfy (36), (37) and

$$(38) \quad \beta \equiv \omega \pmod{P}.$$

Solutions of these additive congruences again exist for the ideals P , Q_1 , Q_2 and α are relatively prime in pairs. Furthermore α and β are again generators of distinct proper extensions by the arguments of the preceding case.

Case 3. Inertness in Z_α and decomposition in Z_β .

This case is always realizable.

Let α satisfy

$$(39) \quad \alpha \equiv \omega \pmod{P},$$

(33) and (34), and let β satisfy (35), (36) and (37). Then K is a desired field by arguments analogous to those in the preceding cases.

Case 4. Decomposition in Z_α , ramification in Z_β .

This case is always realizable.

Let α satisfy (32), (33) and (34). Then α , the conductor of Z_α over F is prime to P , Q_1 and Q_2 . Let $\bar{B}$ in $\bar{Z}_\alpha$ have

¹⁰H. Hasse, op. cit., Part II, pp. 29-40.

the form $P \sum_{i=0}^{p-1} a_i \alpha_1^i R$, where $N(\bar{Z}_\alpha/\bar{F}; R)$ is a unit in $\bar{F}$, and α_1 are integers so selected that $\sum_{i=0}^{p-1} \alpha_1^i = 1$. Then $N(\bar{Z}_\alpha/\bar{F}; \bar{B})$ has P_α -adic value 1. Hence we can always select a B in Z_α , such that $N(Z_\alpha/F; B)$ has P -adic value 1. Now let $\beta = \zeta N(Z_\alpha/F; B)$. Then β is a prime element for P . Thus Z_β is a proper extension and P ramifies in Z_β . Since P decomposes in Z_α by (32), $Z_\alpha \neq Z_\beta$, and K is a desired field.

Case 5. Inertness in both Z_α and Z_β .

This case is always realizable.

Let α satisfy (39), (33) and (34), and β satisfy (38), (36) and (37). The arguments are analogous to those in Cases 1, 2 and 3.

Case 6. Ramification in both Z_α and Z_β .

This case is always realizable.

Note that in this case α must be a prime element for P . Thus let $\alpha = \pi_1$. Then Z is a proper extension. Consider the local properties of the field Z_α . The roots of unity in $\bar{Z}_\alpha$ and in $\bar{F}$ are the same, and $x = \sqrt[p]{\alpha}$ is a primitive element of $\bar{Z}_\alpha$. Then the general element¹¹ of $\bar{Z}_\alpha$ has the form

$$(40) \quad \Lambda_p = \pi^{r/p} \omega^s u, \text{ where } u \equiv 1 (P_\alpha), s \neq t.$$

Now choose a quantity B in Z_α which is an approximation for $A = \pi^{r/p} \omega^s$ in $\bar{Z}_\alpha$ where $r \equiv 0 \pmod{P}$. Then let $\beta = \zeta N(Z_\alpha/F; B)$. Then the P -adic value of β is 1 in F , $Z_\alpha \neq Z_\beta$, and P ramifies in Z_β by Lemma 3.

¹¹K. Hensel, Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines Primteilers, Journal für Mathematik, vol. 146 (1916), pp. 189-215.

Case 7. Ramification in Z_α , decomposition in Z_β .

This case is realizable if and only if ζ is in $(\overline{F}')^P$.

Again as in Case 6 α must be a prime element for P. The general quantity of $\overline{Z}_\alpha$ is again A_p as in the preceding case. To insure extensibility we must take $\beta = \zeta N(Z_\alpha/F; B)$ where B is an approximation in Z_α of A_p . Then β has the form $\zeta \pi^r \omega^{sp}$. But to be a generator of a decomposition field for P, the element β must be in $(\overline{F}')^P$. Thus we must have $r \equiv 0 \pmod{p}$, and hence ζ must be a p-th power in $\overline{F}$. This proves the necessity of the condition.

Now let ζ be in $(\overline{F}')^P$. Let $\alpha = \pi$ and let β satisfy (36) and (37). Then K is a desired field.

Case 8. Ramification in Z_α , inertness in Z_β .

This case is realizable if and only if ζ is not in $(\overline{F}')^P$.

Here again $\beta = \zeta N(Z_\alpha/F; B)$ where B is taken as in the preceding case. But now clearly P remains inert in Z_β if and only if ζ is not a p-th power in $\overline{F}$, and $r \equiv 0 \pmod{p}$. This is true if and only if ζ does not lie in $(\overline{F}')^P$. The sufficiency argument is as in the preceding case.

Case 9. Inertness in Z_α , ramification in Z_β .

This case is never realizable.

Suppose K is an extensible field having the arithmetic prescribed in this case. We shall show that this assumption leads to a contradiction.

By Lemma 2 we have

$$(41) \quad \alpha = \omega^i d^p \text{ with } i \not\equiv 0 \pmod{p}, \quad d^p \text{ in } (\overline{F}')^P.$$

Consider the local structure of Z_α . Since P is inert in Z_α , π_α is a prime element in $\overline{Z}_\alpha$. Let ω be a primitive $(q^p - 1)$ st root of unity in $\overline{Z}_\alpha$. Then $N(\overline{Z}_\alpha/\overline{F}; \omega) \equiv \omega(P)$. The general element

of $\overline{Z}_\alpha$ now has the form

$$(42) \quad A_p = \prod_0^{\mathbb{P}} \omega_0^{\mathbb{S}} u \quad \text{where } u \equiv 1 \pmod{p_\alpha}.$$

Then $N(\overline{Z}_\alpha/F; A_p) = \prod_0^{\mathbb{P}} \omega_0^{\mathbb{S}} N(\overline{Z}_\alpha/F; u)$ and $\beta = \int \prod_0^{\mathbb{P}} \omega_0^{\mathbb{S}} N(\overline{Z}/F; u)$. Hence the P -adic value of β is divisible by p . This contradicts our previous assumption that P is ramified in Z_β . Therefore this case is impossible.

REMARK. We shall show below that there exists no Hilbert series for P_L in L which induces the arithmetic of Case 9 in K/F . Thus this case is excluded by the Hilbert Theory. This fact, however does not follow from the investigation of the Hilbert series of K/F and must be deduced from extensibility conditions.

Thus we see that with the exception of the last case which is altogether excluded, and cases seven and eight, which are realizable only under certain mutually exclusive conditions, every type of factorization of P in K is realizable. We shall now say that K is of type 1 with respect to a prime ideal P if P factors in K as in Case 1 above. We shall now prove the following existence theorem.

THEOREM 6. Let $P_{1,1}, P_{1,2}, \dots, P_{1,s_1}; P_{2,1}, \dots, P_{2,s_2}; \dots, P_{8,1}, \dots, P_{8,s_8}$ be a finite set of prime ideals of F , and let $\mathcal{S}$ be contained in $(\overline{F}')_{7,j}^p$ ($j = 1, \dots, s_j$) but not in $(\overline{F}')_{8,j}^p$ ($j = 1, \dots, s_8$). Then there exist fields $K = Z_\alpha \cup Z_\beta$ over F extensible to L such that K is of type 1 with respect to $P_{1,1}, \dots, P_{1,s_1}$ ($i = 1, \dots, 8$).

Proof. Let Q_1 and Q_2 be distinct prime ideals of F not contained in the set $\{P\}$. Let π_{1j} be prime quantities of F associated with the prime ideals P_{1j} and ω_{1j} the associated roots of unity. Consider the system of simultaneous additive congruences

$$\begin{aligned}
 (43) \quad & \alpha \equiv 1 \ (P_{1,j}) \quad j = 1, \dots, s_1, \\
 & \alpha \equiv 1 \ (P_{2,j}) \quad j = 1, \dots, s_2, \\
 & \alpha \equiv \omega_{3,j} \ (P_{3,j}) \quad j = 1, \dots, s_3, \\
 & \alpha \equiv 1 \ (P_{4,j}) \quad j = 1, \dots, s_4, \\
 & \alpha \equiv \omega_{5,j} \ (P_{5,j}) \quad j = 1, \dots, s_5, \\
 & \alpha \equiv \pi_{6,j} \ (P_{6,j}^2) \quad j = 1, \dots, s_6, \\
 & \alpha \equiv \pi_{7,j} \ (P_{7,j}^2) \quad j = 1, \dots, s_7, \\
 & \alpha \equiv \pi_{8,j} \ (P_{8,j}^2) \quad j = 1, \dots, s_8, \\
 & \alpha \equiv \varepsilon_1 \ (Q_1), \\
 & \alpha \equiv 1 \ (Q_2).
 \end{aligned}$$

The system has a solution, since the moduli are relatively prime in pairs. We accordingly choose a solution as a generator of the field Z . Then by previous constructions; Z is a proper extension, and each prime ideal P_{ij} has the desired factorization in Z by Lemma 2.

Next we construct a quantity A in Z as follows

$$(44) \quad A = \left[\prod_{i=0}^{p-1} \prod_{j=1}^{s_4} (\pi_{\alpha})_{4,j}^{s_1 \alpha_i} \right] \prod_{j=1}^{s_6} \pi_{6,j} \omega_{6,j} \prod_{j=1}^{s_7} \pi_{7,j}^p \omega_{7,j} \prod_{j=1}^{s_8} \pi_{8,j}^p \omega_{8,j}.$$

Let now β be a solution of the following additive congruences.

$$\begin{aligned}
 (1) \quad & \beta \equiv \zeta N(Z_{\alpha}/F, A) \bmod \alpha, \\
 (ii) \quad & \beta \equiv \zeta N(Z_{\alpha}/F, A) \bmod P_{4,j} \quad j = 1, \dots, s_4, \\
 (45) \quad (iii) \quad & \beta \equiv 1 \bmod \prod_{j=1}^{s_1} P_{1,j} \cdots \prod_{j=1}^{s_3} P_{3,j}, \\
 (iv) \quad & \beta \equiv 1 \ (Q_1), \\
 (v) \quad & \beta \equiv \varepsilon_2 \ (Q_2).
 \end{aligned}$$

These are again additive congruences with relatively prime moduli. Then if β is a solution of (45), the extensibility of $K = Z_{\alpha} \cup Z_{\beta}$ is insured by (i), the desired factorization of β is insured by

(ii) - (iii), while (iv) and (v) imply that Z_β is a proper extension distinct from Z_K .

To establish an analogous theorem for the case of group G' , note that K is extensible to L with group G' if α is arbitrary and $\beta \equiv 1 (\alpha)$. We repeat the arguments of the previous constructions substituting

$$(36') \quad \beta \equiv 1 (\alpha)$$

for (36) throughout. Then Cases 1' - 6' are unconditionally realizable, and so is Case 7', for in that case β must be in $(\overline{F}')^P$ if and only if it is not a prime element for P . Then clearly Case 8' is excluded. Case 9' is likewise excluded as above. We shall show below that these two cases are also excluded by the Hilbert Theory.

THEOREM 6'. Let P_{1j} be a finite set of prime ideals as in Theorem 6. Then there exist extensible fields K extensible to L with group G' of type 1 with respect to $P_{11}, \dots, P_{1s_1}$ ($i = 1, \dots, 7$).

7. Arithmetic of the non-abelian field.—It remains to examine the possible types of factorization of P_K in L . Since all the possible induced arithmetics in K/F have been discussed, it remains to examine the behavior of the prime ideals P_K , the prime divisors of P in K , in each of the eight possible types of K if L has group G and seven cases if L has group G' .

Let P_K be one of the conjugate prime factors of P in an extensible field K/F . Then P_K may factor further as follows in the cyclic extension L/K :

- (i) P_K may decompose totally in L ,
- (ii) P_K may remain inert in L ,
- (iii) P_K may ramify in L .

LEMMA 3. If P_K factors in L/K as in (i), (ii) or (iii) above, then all its conjugates factor in the same fashion.

Proof. Since L is a normal extension of F , the conjugates of the prime factors of P_K in L have to exhaust the set of all conjugate factors of P in L . Thus the relative degrees and ramification orders of all factors of P relative to K are the same. This proves the lemma.

We remark that it suffices then to investigate a typical factor P_K of P for its factorization type in L . In other words it remains to apply the results of Lemma 2 to the generator $\mathcal{O}$ of L/K and to P_K .

In the sequel we shall discuss separately the possible types of K with respect to P_K as to the possible further factorization of P in L . Some such possibilities will be excluded a priori by means of the Hilbert Theory.

Type 1. Decomposition in Z_α and in Z_β .

Decomposition, inertness, ramification of P_K in L are all realizable.

We remark first that the Hilbert Theory does not exclude any of the three factorizations above. The decomposition fields of any of the conjugate prime divisors of P in L must contain the abelian field K/F .

Suppose now that $\mathcal{O}$ is a generator of some fixed L/K , which exists by the construction of K of type 1. Then by Theorem 5, $\mathcal{O}c$ for any $c \neq 0$ in F are the generators of the set of all fields L containing K and having G as Galois group. By Lemma 2 it suffices to find elements c in F such that $c\mathcal{O}$ has the desired local behavior at any of the prime divisors P_K of P . Such c evidently exist for π and ω are in F .

Type 2. Decomposition in Z_α , inertness in Z_β .

Decomposition of P_K in L is always realizable. Inertness is never realizable. Ramification is always realizable.

We note that inertness of P_K in L is excluded by the Hilbert Theory, since otherwise L is the inertial field for P and must be cyclic over the decomposition field Z_α , whereas it is evident from the lattice of subfields (cf. Section 1) that L is of type (p, p) over Z_α . We shall now show that if decomposition is possible, so is ramification, and vice versa. For π in F is a prime quantity in K , and if γ is a generator of L in which P has one type of factorization, we select $c\gamma$ where $c \equiv \pi^t \pmod{p^2}$ with a properly chosen integer t . Then the element $c\gamma$ will have, by Lemma 2, the desired properties.

Type 3. Inertness in Z_α , decomposition in Z_β .

Decomposition in L is unrealizable. Both inertness and ramification are realizable.

Decomposition is excluded by the Hilbert Theory since otherwise the decomposition field for P_L would be of degree p^2 over F and it would contain Z_β , whereas no such subfield of L exists. Moreover π is again a prime quantity in K , and hence both the remaining types of factorization are realizable by the arguments of the preceding case.

Type 4. Decomposition in Z_α , ramification in Z_β .

Decomposition and inertness are both realizable. Ramification is not realizable.

Ramification is excluded, since otherwise Z_α would be the inertial field for P , and L would have to be cyclic over Z_α , whereas by Section 1, L is of type (p, p) over Z_α . Moreover the $(q-1)$ st root of unity of $\bar{F}$ is primitive in K . Therefore by selecting $c\gamma$

where $c \equiv \omega^t (p)$ for a proper integer t , both possible factorizations are realizable.

Type 5. Inertness in both Z_α and Z_β .

Decomposition is realizable. Inertness is unrealizable.

Ramification is realizable.

Note that in this case P_K cannot be prime in K , since otherwise K would be cyclic over F . Therefore P_K must be partially decomposed in K , that is P is totally decomposed in some subfield of L of degree p over F . From the lattice of subfields, we see that L is not cyclic over any of these subfields. Hence L cannot be the inertial field for P_L . Moreover since π is prime in K , both of the remaining types of factorization are possible by previous arguments.

Type 6. Ramification in both Z_α and Z_β .

Decomposition is realizable. Inertness is realizable.

Ramification is not realizable.

Since P_K cannot be totally ramified in K , it must either decompose or remain inert in one of the subfields of K . However it cannot remain inert in such a subfield, for the structure of L over all of them is the same as over Z_α . Thus we would have by proper change of generators the same situation as in case 9, which was excluded in the preceding section. Therefore P_K must decompose in some subfield of K . Thus the $(q-1)$ st root of unity in $\bar{F}$ is primitive in K , and if decomposition is possible, so is inertness.

Type 7. Ramification in Z_α , decomposition in Z_β .

Ramification only is realizable.

Both decomposition and inertness are excluded since otherwise there would exist a decomposition field or an inertial field of degree p over F and containing Z in contradiction to the structure of L .

Type 8. Ramification in Z_α , inertness in Z_β .

Ramification only is realizable.

Decomposition is excluded since otherwise P would be partially decomposed in K , whereas it is partially ramified in K . Inertness is excluded since otherwise there would exist an inertial field of degree p^2 over F and containing Z_β . Hence ramification only is possible.

At this point we can show how Case 9 is excluded by the Hilbert Theory. This case presupposes inertness in Z and ramification in Z_β . But if L/K exists, the P_K has one of the three possible factorizations in L . But decomposition is impossible since otherwise P_K would be partially decomposed in K ; inertness is impossible since otherwise there would exist a cyclic inertial field of degree p^2 over F , whereas no such cyclic subfield of L exists; ramification is impossible since otherwise L would be cyclic over Z_α . Thus we are led to a contradiction. Therefore no field L/K exists, and evidently the arithmetic of Case 9 is incompatible with extensibility conditions.

It is also interesting to point out that it is possible to exclude the cases excluded by Hilbert Theory by considering the local structure of the subfields. As an example, we choose K of type 2. Here, as we have seen above, inertness of P_K in L was excluded by Hilbert Theory. Now $L = K(z)$ where $z^p = \gamma$ in K . Also $P_K = P_\alpha$ in this case. Now if $P_L = P_K = P_\alpha$, we must have $\gamma = d^p \Omega^1$ where Ω is the $(q^p - 1)$ st root of unity in $\bar{K}$, d in $\bar{K}$. Furthermore $\bar{K} = \bar{Z}_\alpha(\Omega)$, and Ω is a root of a pure equation in $\bar{Z}_\alpha$. Consequently $\Omega = y^r f$ where f is in $\bar{Z}_\alpha = \bar{F}$. Also b is the generating automorphism of $\bar{K}$ over $\bar{F}$. We now have $\gamma = d^p f y^r$. By Theorem 1, $\gamma^b \gamma^{-1} = (d^p)^b (d^p)^{-1} \gamma = \mathcal{M}^p$. But then $\mathcal{M} = d^{b-1} \sqrt[p]{\gamma}$,

$N(K/Z_\infty; \lambda) = \zeta$ contrary to Theorem 1. Therefore the prescribed arithmetic of L is incompatible with the extensibility conditions.

3. The general existence theorem.

THEOREM 7. Let $P_{1,j}$ be a finite set of prime ideals of F as in Theorem 6. Then there exist fields L of degree p^3 over F such that any prescribed arithmetic of L with respect to each of these ideals, which is not excluded by Hilbert Theory, is realizable.

Proof. We shall indicate an actual construction of L for any prescribed arithmetic with respect to the set $P_{1,j}$.

To begin with, such a prescribed arithmetic induces an arithmetic in K/F , which is as in Theorem 6. We next construct K as in that theorem. Then each of the ideals of the set $P_{1,j}$ has the desired behavior in K . Then K is of type 1 with respect to the ideals $P_{1,j}$ ($j = 1, \dots, s_1$). By the construction of Theorem 6, K is extensible, and there exists some generator γ of L in K . Let us construct an arbitrary $L = K(z)$ with $z^p = \gamma$. Then the factorization of the ideals $P_{7,j}$ and $P_{8,j}$ is determined in L . Suppose none of the ideals factors as desired in L . Then choose a root of the system of congruences

$$\begin{aligned}
 c &\equiv \pi_{1,j}^{t_j} (P_{1,j}^2) & j = 1, \dots, r, \\
 c &\equiv \omega_{1,k}^{t_k} (P_{1,k}) & k = r+1, \dots, s_1, \\
 c &\equiv \pi_{2,j}^{t_j} (P_{2,j}^2) & j = 1, \dots, s_2, \\
 (46) \quad c &\equiv \pi_{3,j}^{t_j} (P_{3,j}^2) & j = 1, \dots, s_3, \\
 c &\equiv \omega_{4,j}^{t_j} (P_{4,j}) & j = 1, \dots, s_4, \\
 c &\equiv \pi_{5,j}^{t_j} (P_{5,j}) & j = 1, \dots, s_5, \\
 c &\equiv \omega_{6,j}^{t_j} (P_{6,j}) & j = 1, \dots, s_6,
 \end{aligned}$$

where the integers t_j are as in the construction of L in the preceding section. These are additive congruences and the moduli are relatively prime. Thus a solution c exists. Note that c is locally not a p -th power and hence it is not a p -th power in F . Neither is it a p -th power in K since otherwise $c\mathcal{O}$ would generate the same field over K as $\mathcal{O}$, whereas by construction the prime ideals acquire a different factorization in L . Then the field $L = K(\sqrt[p]{c\mathcal{O}})$ has the desired arithmetic by the previous constructions and is a normal extension of degree p^3 over F by Theorem 5. This proves the theorem.

We conclude by stating the analogous results for the case when L has group G' as Galois group. The following are the realizable factorizations of the prime ideal P in L .

Type 1'. Decomposition, inertness or ramification.

Type 2'. Decomposition or ramification.

Type 3'. Decomposition or ramification.

Type 4'. Decomposition or inertness.

Type 5'. Decomposition or ramification.

Type 6'. Decomposition or inertness.

Type 7'. Decomposition or inertness.

Type 8'. Excluded.

Type 9'. Excluded.

THEOREM 7'. There exist fields L with Galois group G' over F with any prescribed arithmetic not excluded by the Hilbert Theory with respect to any finite set of prime ideals P_{1j} of F .

VITA

Anatol Rapoport was born in Lozovaya, Russia, on May 22, 1911. He came to the United States in 1922 and graduated from Tuley High School, Chicago, in 1927.

In January, 1937, he entered the University of Chicago where he received his Bachelor of Science degree in June, 1938, and his Master of Science degree in June, 1940. He did his graduate work in mathematics under Professors Albert, Barnard, Bartky, Bliss, Dickson, Graves, Hestenes, Lane, Reid and Schilling. He wishes to express his gratitude to all of them and feels particularly indebted to Dr. Schilling for his kind assistance and guidance in the preparation of this thesis.

